anand guru

SOC EXPERTS

Interview Questions on **Threat Intelligence**

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is Threat Intelligence?

- Threat intelligence is knowledge that allows organization to prevent or mitigate cyberattacks esp. zero-day malwares or exploits.
- It is a subscription based services offered by many vendors.
- Technically TI is a database of Indicators of Compromise.

anand guru

Name few open source Threat Intelligence feeds.

- Abuse.ch
- OSINT
- threatfeeds.io
- autoshun.org
- malwaredomainlist.com

anand guru

Name few commercial Threat Intelligence feeds.

- IBM X-Force Exchange
- Anomali ThreatStream
- Palo Alto Networks AutoFocus
- FireEye iSIGHT Threat Intelligence
- Recorded Future

anand guru

What is an IOC?

- IOC Stands for Indicators of Compromise. Its an attribute (forensic data) associated with an attack.
- IOC focuses on what of an attack.
- Attributes associated with an attack might include - **IP address, URL, email, file hash etc.**

anand guru

What is IOA?

- IOA stands for Indicators of Attack.
- IOAs focus more on the WHY and intent of an actor.
- IOA is some events that could reveal an active attack before indicators of compromise become visible. Like, unknown process running
- Unlike Indicators of Compromise (IOCs) used by legacy endpoint detection solutions, indicators of attack (IOA) focus on detecting the intent of what an attacker is trying to accomplish.

anand guru

What Are the Common Indicators of Compromise obtained from Threat Intelligence?

- **IP addresses, URLs and Domain names**: An example would be malware targeting an internal host that is communicating with a known threat actor.
- **Email addresses, email subject, links and attachments**: An example would be a phishing attempt that relies on an unsuspecting user clicking on a link or attachment and initiating a malicious command.
- **Registry keys, filenames and file hashes and DLLs**: An example would be an attack from an external host that has already been flagged for nefarious behavior or that is already infected.

anand guru

What security solutions use Threat Intelligence?

- In todays world almost every prevention and detection system use TI feeds.
- AV solutions can use to check the malicious hashes
- Firewall can use TI to check blacklisted IP etc.

anand guru

How does Threat Intelligence work?

Threat Intelligence Works in 2 ways

- Few TI feeds let you download the IOC database on-prem (like integrating into SIEM lists)
- Few other TI, works as a subscription based, every time you need to check the reputation of a file, URL or IP address, the security solution makes a quick light-weight query to the TI server, get the responses and take appropriate actions.

Where do you install Threat Intelligence in the network?

This is a trick question.

- TI is not installed on-prem, it is a subscription based services offered by many vendors.

anand guru

Why Is Threat Intelligence Important?

- TI helps to keep companies informed of the advanced threats, exploits and zero-day threats that they are most vulnerable to and how to take action against them.

anand guru

What is US-CERT?

- It is a website maintained by US Department of Homeland Security. It is a good source of TI.
- US-Cert release information about new threats in the form of Technical Alerts

anand guru

Example of how you have consumed TI?

- Integrating TI feeds with SIEM
- Using IPVoid , URLVoid or VirusTotal during analysis of any alert
- Ad-hoc reports for latest attacks (using their IOCs)

anand guru

How TI can be integrated with SIEM?

- TI can be integrated using Lists. These lists should be updated regularly to get the latest IOCs

anand guru

What are TAXII and STIX?

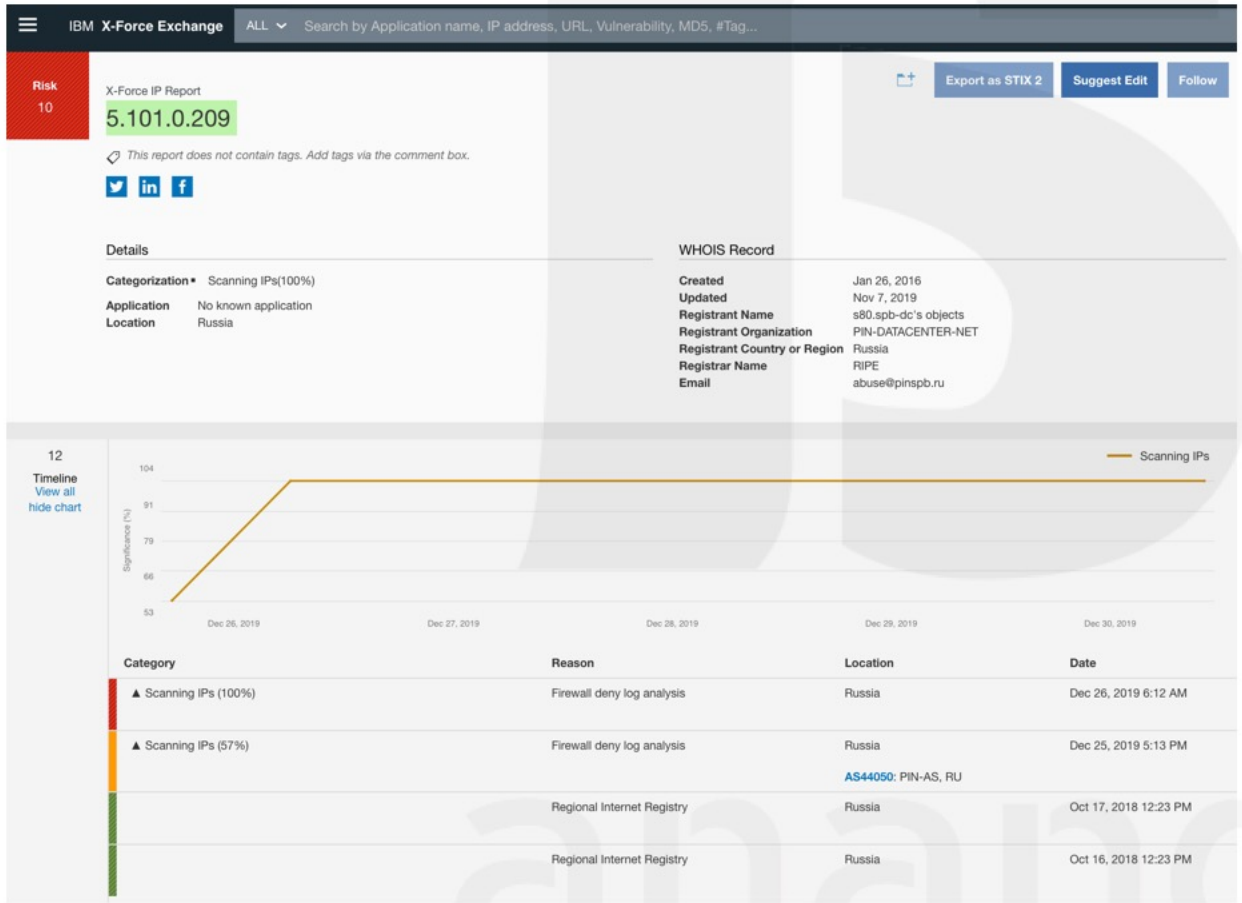
- Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).
- Structured Threat Information eXpression (STIX) is a structured language for cyber threat intelligence

- Trusted Automated eXchange of Indicator Information (TAXII™) is a free and open transport mechanism that standardizes the automated exchange of cyber threat information.
- A transport mechanism for sharing cyber threat intelligence
- Example: http://hailataxii.com/

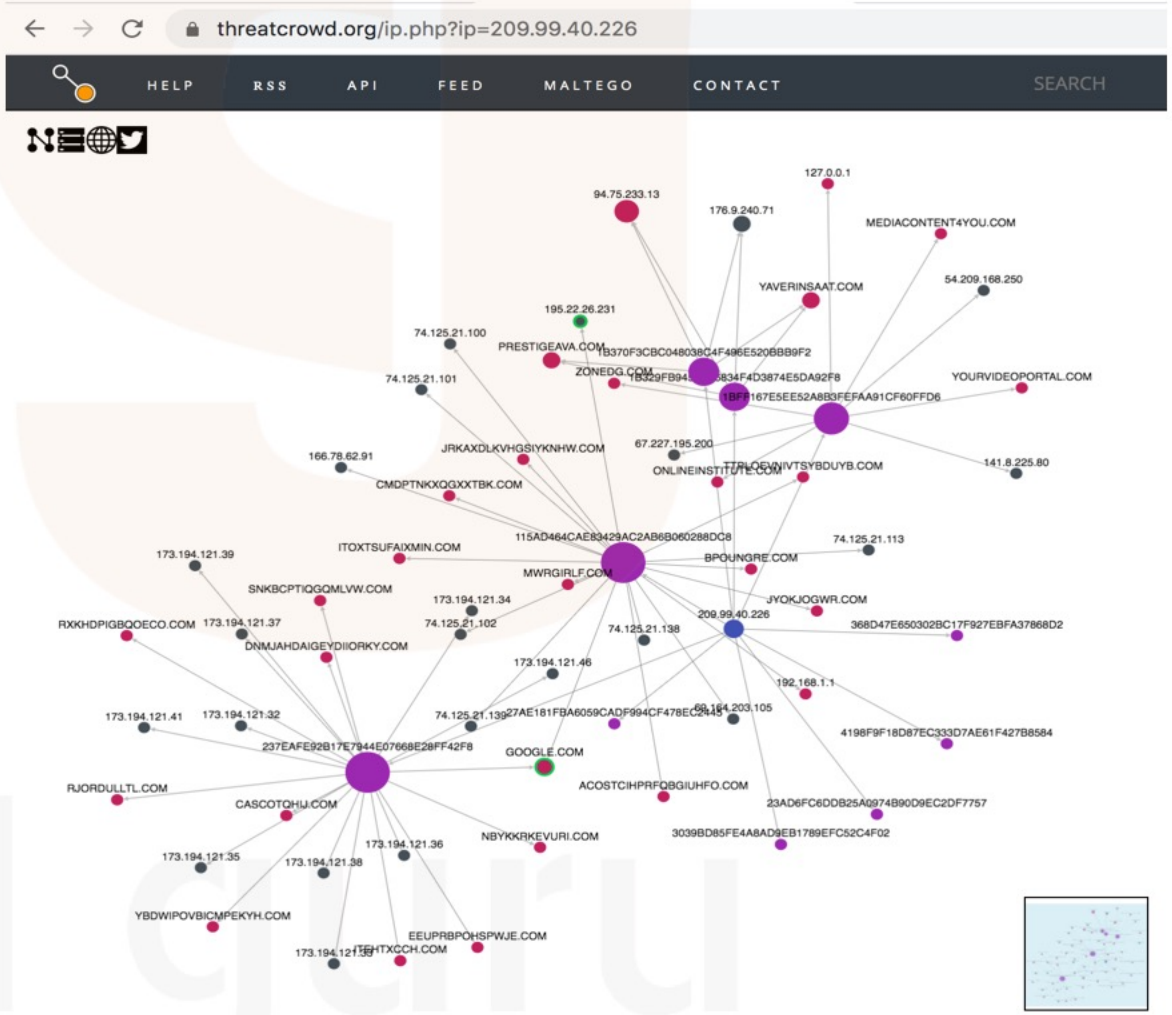
STIX states the what of threat intelligence, while TAXII defines how that information is relayed. STIX and TAXII are machine-readable and therefore easily automated.

Which is you favorite TI?

- IBM X-Force
  - Provides an exact score
  - Gives a timeline of how the IP was behaving over a period of time



- Threat Crowd
  - Gives a graphical representation of association of various attributes like domain name, IPs and file hashes



anand guru

Full course on Udemy

IT & Software › Network & Security › Cyber Security

SOC Analyst (Cybersecurity) Interview Questions and Answers

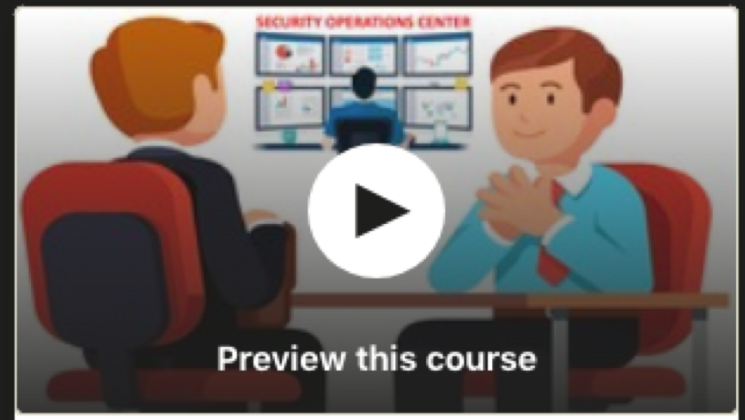
Clear your next SOC interview with ease with these 300+ interview question asked during most SOC Analyst Interview

Bestseller 4.6 ★★★★½ (106 ratings) 2,248 students

Created by Anand Guru

Last updated 5/2020 English English

Wishlist Share Gift this course



₹455 ~~₹1,280~~ 64% off

5 hours left at this price!

Add to cart

Buy now

30-Day Money-Back Guarantee

What you'll learn

- ✓ Security Analyst/SOC Analyst interview questions and how to answer them
- ✓ Tricky questions and how to answer them
- ✓ Scenario based questions
- ✓ SOC Analyst Training
- ✓ Wide range of topics covered in a SOC Interview
- ✓ How to answer experience related questions
- ✓ Ready-to-use sample CVs for SOC Analyst role

This course includes:

- 2.5 hours on-demand video
- 2 articles
- 8 downloadable resources
- Full lifetime access
- Access on mobile and TV
- Certificate of completion